# ¿Las cadenas de bloques tienen algo que ofrecer a la identidad?

22 febrero de 2018

## Introducción

**Autores**
Steve Olshansky
Internet Society

Steve Wilson
Lockstep Consulting
Steve Wilson es un investigador independiente, innovador, asesor y analista de identidad y privacidad digital.
Ver http://lockstep.com.au

**Asistente**
Robin Wilton
Internet Society

Creamos este artículo porque la gestión de identidad y acceso (Identity and access management (IAM) se han convertido en una parte esencial de nuestras interacciones en línea. Al igual que gran cantidad de infraestructura, cuando está bien diseñada e implementada, la IAM es mayormente invisible para los usuarios. Debido a ello, muchas personas que no están activamente involucradas en el tema no conocen por completo su generalidad y su impacto en nuestras vidas cotidianas.

La cadena de bloques es una clase general de métodos relativamente nuevos de seguridad de los datos, con ciertas propiedades de valor potencial en la IAM. La cadena de bloques proporciona gran emoción. Numerosas compañías de emprendimientos de IAM han lanzado soluciones de registro de identidad "en la cadena de bloques", en tanto que otras desarrollan nueva infraestructura inspirada en la cadena de bloques para distribuir atributos, un elemento clave de la IAM. Al enfrentar una cantidad creciente de entusiasmo y escepticismo asociado, nuestro objetivo es proporcionar una perspectiva balanceada, y aclarar las formas en que las tecnologías de cadena de bloqueos pueden o no cumplir con las necesidades de la IAM. Tal vez, lo que es más importante, esperamos proporcionar una perspectiva útil para evaluar las soluciones actuales y nuevas de IAM basadas en la cadena de bloques a medida que aparecen.

Al analizar cómo estas tecnologías existentes pueden ayudar con la IAM, el punto inicial debe ser apreciar la intención de las primeras cadenas de bloques, y luego presentar un desarrollo con criterios precisos sobre los sistemas. Así, el artículo debe ayudar a quienes crean nuevas soluciones de IAM, y a quienes pueden adquirir soluciones y necesitan evaluar nuevos enfoques basados en la cadena de bloques.

Este artículo está destinado al personal y dirección de tecnología de la información, y toda otra persona que trabaje con tecnologías de IAM y que sienta curiosidad sobre la cadena de bloques y cómo puede afectar la IAM. En primer lugar, presentamos antecedentes sobre la cadena de bloques luego sobre la IAM y luego recomendaciones para relacionarlos.

## Resumen

La IAM se ha convertido en una infraestructura esencial para nuestras interacciones en línea. Evoluciona rápidamente, los intereses son altos y las empresas enfrentan un paisaje de identidad digital cada vez más complejo y desconocido. Existe una creciente preocupación de que numerosas empresas digitales saben mucho sobre nosotros, y el control sobre la identidad debe ser reclamado por los usuarios finales de alguna forma. Entonces, la IAM es un tema actual, con nuevas arquitecturas, modelos de negocios y filosofías, todo en juego.

La tecnología de la cadena de bloques[1] genera atención, positiva y negativa, y una gran emoción. Los defensores proponen su uso para una amplia variedad de casos, incluida la IAM.

La cadena de bloques surgió en un momento crítico, con un conjunto de promesas relacionadas con la seguridad, muchas de ellas aparentemente de aplicación a la identidad, pero de forma superficial. Numerosas empresas de IAM han optado por la "cadena de bloques", y se han formulado declaraciones generales de que esta nueva familia de soluciones interferirá con la IAM tradicional. Si bien los casos de uso y requisitos varían, simplemente agregar las tecnologías de la cadena de bloques a un sistema de IAM sin una consideración atenta de todos los factores no generará necesariamente una mejora real y, de hecho, puede tener el efecto opuesto. Al igual que cualquier tecnología, las cadenas de bloques son simplemente herramientas, para ser consideradas atentamente en el contexto de su entorno en particular. Este artículo presenta una variedad de cuestiones de análisis y diseño a considerar al aplicar las tecnologías de la cadena de bloques a la IAM, en consulta con el personal técnico correspondiente.

Este artículo está destinado a explorar imparcialmente la adaptabilidad entre la tecnología de la cadena de bloques y la IAM para casos de uso de identidad personal. Analizamos la evolución de la cadena de bloques y su aplicación a la IAM, distinguimos los aspectos relevantes del espacio del problema e identificamos asuntos clave a tratar al considerar la cadena de bloques. Las tecnologías de cadena de bloques evolucionan rápidamente, y se debe esperar que cambie la adaptabilidad para la IAM, pero en esta etapa ciertamente no hay necesidad de apurarse, y ninguna razón para temer perderla. Demostramos que las cadenas de bloques originales en general no son una buena opción para la gestión de identidades, e intentamos analizar, en esta etapa inicial, en qué medida los nuevos desarrollos de cadenas de bloques podrían cumplir las necesidades de la IAM.

Suponemos familiaridad con la IAM y la cadena de bloques. Cualquier persona interesada en obtener más información sobre cualquiera de estos temas, puede encontrar buenas referencias en la lista que se incluya el final.

1 En el momento de la redacción, la terminología de este nuevo campo aún está en desarrollo. Para los fines de este artículo, usamos el término "cadenas de bloques" ampliamente para hacer referencia a las cadenas de bloques distribuidas públicas creadas para Bitcoin y otras criptomonedas, y desarrollos más recientes, en ocasiones conocidos como tecnologías distribuidas o compartidas.

## Cadena de bloques, cadenas de bloques y "libros distribuidos"

¿Por qué la cadena de bloques (o, más en general, las "tecnologías de cadena de bloques") se promociona como una solución útil para los problemas actuales en la IAM en línea? Si bien hay un gran entusiasmo asociado y actualmente las personas procesan su uso en una variedad de entornos, existen asuntos particulares para la identidad que algunos consideran que se pueden resolver con los algoritmos de la cadena de bloques y los lanzamientos relacionados.

### Las características y propiedades de seguridad de las tecnologías relacionadas con la cadena de bloques en evolución

| **Cadenas de bloques públicos de primera generación**<br>por ej., Bitcoin, Ethereum | **Tecnologías de cadenas de bloques avanzadas/de propósitos especiales**<br>por ej., Corda, Fabric, Plenum, Hashgraph |
|---|---|
| Redes altamente distribuidas, altamente descentralizadas | Tienden a ser más concentradas: menor número de participantes o nodos |
| Sin permisos | Controles de acceso de escritura o lectura |
| Redes públicas de nodos entre pares | Puede ser una red privada física o virtual |
| Inmutable por el peso real de los números en la red | Con un grupo más reducido de participantes, la resistencia a la manipulación puede requerir seguridad tradicional en los nodos |
| Fuente libre y abierta | Puede ser software de propiedad exclusiva y una red comercial |

La cadena de bloques original fue desarrollada para resolver un problema en particular: el "doble gasto" de la criptomoneda sin un administrador central. El problema intrínseco con la moneda puramente virtual es que nada previene inherentemente que el dinero se duplique: se requiere cierta forma de supervisión para prevenir el doble gasto. Si bien varios esquemas de dinero electrónico han existido por décadas (uno de los primeros es *Digicash* fundado en 1989), siempre tuvieron una autoridad central para controlar el doble gasto. La cadena de bloques permitió que opere la primer criptomoneda entre pares, principalmente Bitcoin, sin intermediarios y sin un "banco de reserva" digital. Una red pública masiva supervisa cada movimiento de Bitcoin, y mantiene un libro en constante crecimiento con solo apéndices (la cadena de bloques) de cada transacción realizada. Los nodos de red ejecutan el software de cadena de bloques de fuente abierta y son recompensados por su participación mediante asignaciones aleatorias de Bitcoin.[2]

La cadena de bloques original de Bitcoin está altamente distribuida,[3] sin un único punto de control (o falla) y no se puede alterar una vez que se escribió. Al ser descentralizada,

2 No debemos preocuparnos por los detalles aquí, pero en breve, ciertos nodos "completos" de la red Bitcoin son recompensados por el pago de un botín que luego se asigna al primer nodo que completa una tarea de "prueba de trabajo" de fuerza brutal, cuya dificultad vuelve el libro inmune a la manipulación y falsificación. La probabilidad de ganar el botín aumenta con la cantidad de potencia de cómputo asignada a la tarea, la ejecución de un nodo completo se denomina "minería".

3 Tenga en cuenta que existen varios aspectos de la descentralización en las tecnologías de cadenas de bloques, y que el grado de descentralización imaginado por sus diseñadores originales no ha sido uniforme. El tema es demasiado amplio para cubrir en cualquier medida en este artículo, pero en breve, las arquitecturas de cadenas de bloque pueden descentralizar el *almacenamiento y disponibilidad* del libro o el *proceso para alcanzar el consenso* sobre el estado del libro. Se esperaba que el último, conocido como "minería" en las cadenas de bloques públicas, se mantenga altamente distribuido y resistente a la corrupción, pero resultó que la minería de Bitcoin se volvió tan rentable que ha generado una concentración masiva de esta actividad, y compromisos resultantes en la seguridad de Bitcoin, al menos en teoría. Otro aspecto de la descentralización es la *gobernanza*, que aún debe organizarse correctamente en las cadenas de bloques públicas de Bitcoin y Ethereum. La toma de decisiones sobre importante mantenimiento del software ha resultado difícil o incluso intrincada con Bitcoin, y en ocasiones se ha asignado a solo una persona en Ethereum.

prácticamente inmutable y criptográficamente verificable, este tipo de cadena de bloques parece prestarse a infinitas aplicaciones más allá de los pagos, como la IAM, para reducir el fraude, eliminar los atascos y seguir el origen de complejos datos de partes múltiples. Estas propiedades son importantes para la IAM, por lo que hubo una aceleración en la investigación y desarrollo de la cadena de bloques para IAM, entre muchas otras cosas. Los últimos cuatro o cinco años han presenciado una agitada evolución. El sistema original de Bitcoin y sus derivados estrechamente relacionados representan una clase de cadenas de bloques *públicas*. Los algoritmos descendientes más avanzados, desarrollados para casos de uso más complejo que la criptomoneda, ofrecen diferentes combinaciones de propiedades.

## Autenticación y autorización

Como se señaló anteriormente, la IAM evoluciona rápidamente, los intereses son altos, y las empresas enfrentan un paisaje de identidad digital cada vez más complejo y desconocido. Cuando funcionan bien, la mayoría de los mecanismos de la IAM se mantienen ocultos de los usuarios, que en general están más interesados en un acceso conveniente y confiable a los servicios que ser "identificados" como tales. Las tecnologías móviles con potente criptografía y biometría integrada se han vuelto autenticadores populares. Al mismo tiempo, existe una frustración generalizada y una creciente inquietud de que numerosas empresas digitales saben demasiado sobre nosotros, y que el control de nuestra información y nuestra identidad debe ser reclamado por los usuarios finales de alguna forma.

Al considerar el potencial de interferencia de las tecnologías como la cadena de bloques, es aún más importante aclarar el problema que intentamos resolver. Si se considera que la cadena de bloques tiene el potencial de mejorar la calidad y la disponibilidad de la información sobre las partes con quienes intentamos negociar, entonces primero revisemos de qué se tratan básicamente la autenticación y la autorización.

La pregunta esencial en IAM puede formularse de este modo: en un contexto en particular, ¿qué se necesita saber sobre una contraparte a fin de poder negociar con ella (es decir, aceptar una transacción o artefacto digital de ella)? En la mayoría de los entornos comerciales, es menos importante saber *quién* es alguien que saber *cómo* es. Es decir, por ejemplo, ¿cuál es su calificación profesional? O su membresía en una organización, relación con un proveedor de servicios, país de origen, derecho a recibir servicios del gobierno, vigencia como cliente comercial, o edad, según corresponda. Son los tipos de datos (es decir, atributos) que se usan en las decisiones detalladas (o basadas en atributos) del control de acceso.

Estos tipos de preguntas deben formularse en el momento del diseño, al realizar una evaluación de riesgos de la transacción deseada y analizar los requisitos de autenticación y autorización. Se pueden explorar formas diferentes para que los sistemas de transacciones reciban los atributos necesarios de identidad en el momento correcto, por ejemplo cuando los usuarios se registran para servicios, o cuando realizan transacciones. Esto introduce un nuevo conjunto de decisiones de diseño: la identificación directa al registrarse no necesita ser tan rigurosa, por ejemplo, si hay otras mitigaciones de riesgos (como el puntaje de riesgo en tiempo real para detectar el fraude) disponibles. Al diseñar sistemas de identificación, debemos decidir qué calidad de información se necesita, dónde se obtendrá esa información y cómo se validará.

**Terminología: los participantes principales de la IAM**
El análisis y diseño de la gestión de identidades se basan en un conjunto de participantes o funciones, a saber:

**Sujeto** (o usuario) es la persona o entidad identificada o mencionada en una transacción y que típicamente recibe servicios de acuerdo con su identidad o atributos. Los sujetos típicamente son clientes, empleados, titulares de cuenta, etc.

**Parte confiable (RP**, o proveedor de servicios- SP) es una entidad que realiza transacciones con un sujeto, y proporciona servicios, y habitualmente depende de un tercero para confirmar la identidad o los atributos del sujeto. Los RP típicos son vendedores minoristas empleadores, instituciones financieras agencias del gobierno, servicios, etc.

**Proveedor de identidad (IdP)** es una parte que responde por la identidad de un sujeto de acuerdo con cierto protocolo de identificación acordado. En las arquitecturas clásicas de IAM, el IdP es clásicamente un tercero (como una agencia del gobierno, institución educativa, empleados o servicio de identificación comercial), pero en el negocio convencional, muchos RP como los bancos asumen la responsabilidad por la identificación y, en consecuencia, actúan como sus propios IdP.

**Autoridad/proveedor de atributos** con frecuencia es el IdP pero también puede ser una entidad separada fuera del control directo del IdP. De forma similar, podría haber "agentes de atributos" externos que obtienen y acumulan atributos de una variedad de fuentes. En definitiva, depende del RP tomar una decisión sobre cuánta confianza asignar a las fuentes de atributos.

Algunos entornos de IAM incluyen proveedores de atributos separados e intermediarios adicionales. En general, las partes confiables tienden a asumir la mayor parte del riesgo en una transacción, y habitualmente tienen la decisión final sobre si un protocolo de identificación es adecuado para un propósito o no. Las obligaciones contractuales de los IdP frente a los RP, garantías y acuerdos de responsabilidad son temas eternos de debate en la IAM. En consecuencia, en aplicaciones conservadoras o de mayor riesgo como el gobierno, atención médica y servicios financieros, los RP con frecuencia actúan como sus propios IdP.

## Declaraciones/Atributos/Afirmaciones

En la IAM, lo que necesitamos saber sobre las contrapartes se conoce como declaraciones, atributos o afirmaciones. Numerosas formalidades para la gestión de riesgos, como las reglas de identificación de clientes bancarios, se enfocan en subconjuntos comunes de atributos, como el "nombre legal" de un documento oficial del gobierno, fecha de nacimiento y dirección residencial.

Al enmarcar la IAM para concentrarse en atributos específicos en diferentes contextos, podemos reducir la acumulación de información extraña (que cada vez más representa una responsabilidad para muchas empresas, a la luz de la epidemia de infracción de datos). Se aplica el "Principio de la necesidad de saber"[4], lo que es bueno para la privacidad, mediante la minimización de la recopilación y divulgación de datos. Y la importancia de la autenticación de tecnologías de cadenas de bloques debe ser más clara. De acuerdo con los

4 https://security.berkeley.edu/need-know-access-control-guideline

riesgos involucrados en la aplicación deseada, los diseñadores de IAM deben decidir cuánta confianza se requiere en los atributos presentados (afirmados) por los usuarios. ¿Los datos de declaración propia son suficientes, o se requiere la validación externa por un tercero confiable? El Grupo de Trabajo de Declaraciones Verificables del World Wide Web Consortium (W3C)[5] realiza trabajo promisorio para permitir la verificación externa de las declaraciones, independientemente de su lugar de almacenamiento.

Procedencia

Uno de los temas principales de la IAM ahora es la *procedencia*. Si nos concentramos en los atributos precisos utilizados para autenticar a las personas con quienes negociamos, ¿cómo podemos saber qué atributos son confiables? Es decir, ¿qué necesitamos saber sobre los atributos? Los metadatos más obvios de interés para la autenticación incluyen el emisor del atributo: ¿qué escuela emitió el diploma universitario? ¿La edad de una persona se obtiene de un registro público de nacimientos, un departamento de vehículos automotores (department of motor vehicles, DMV) o una red social? También puede ser importante conocer la edad de un atributo, su fecha de vencimiento, dónde y cómo se almacenó y protegió contra la manipulación, y cómo se relaciona el atributo con el sujeto.

Para algunos atributos personales, existe una fuente de autoridad obvia. Las calificaciones personales, por ejemplo, habitualmente son emitidas por organismos profesionales, y los números de tarjeta de crédito son creados por los bancos de emisión. Pero otras declaraciones, como el empleador y la dirección residencial, pueden provenir de diferentes fuentes. Está surgiendo el concepto de una "economía de atributos" en algunos debates sobre los datos personales[6] y podemos esperar el surgimiento de un mercado discutible de proveedores de atributos. Pero en todos los casos, un atributo es solo tan confiable como nuestra certidumbre sobre su origen y nuestra confianza en la fuente.

## Evolución de la cadena de bloques

Fundamentalmente, los problemas inherentes a la criptomoneda entre pares como Bitcoin son diferentes de los de la gestión de identidades y acceso; estas diferencias deben ser comprendidas antes de intentar comparar las tecnologías de la cadena de bloques con la IAM. Los intentos por solucionar estos problemas para diferentes casos de uso han generado cambios importantes en la forma en que operan y se desempeñan las cadenas de bloques.

Las cadenas de bloques surgieron como una forma novedosa de supervisar ciertas transacciones entre personas que no necesitan conocerse ni confiar en el otro, y que eligen no utilizar un administrador central. En un sentido más general, las tecnologías de la cadena de bloques se pueden usar para establecer consenso sobre el estado de un conjunto de datos compartidos, formado por múltiples contribuciones en tiempo real, sin supervisión central. Con Bitcoin, el consenso se trata específicamente del orden en que se realizan intentos para mover la criptomoneda, a fin de detectar y prevenir los intentos de doble gasto. La capacidad de obtener y registrar consenso sobre el orden de los datos almacenados en un registro puede ser útil en contextos más allá de las criptomonedas, y ha sido uno de los principales impulsores de otros usos propuestos, como la IAM.

5 https://www.w3.org/2017/vc/charter.html

6 https://www.linkedin.com/pulse/youre-become-part-attribute-economy-nathan-kinch

En algunos casos de uso, los participantes de una transacción compleja son competidores (como bancos comerciales o compañías farmacéuticas) o provienen de sectores diferentes sin una supervisión común (como diversos transportistas y proveedores que participan en el comercio internacional). Las tecnologías de cadenas de bloques prometen optimizar la forma en que los conjuntos de datos transaccionales como manifiestos de comercio, registros de la cadena de suministro y complejos acuerdos financieros se ensamblan y liquidan en tiempo real.

La criptomoneda entre pares es una aplicación altamente especializada, con suposiciones y restricciones inusuales de diseño. A medida que surgieron casos de uso más complejos para las cadenas de bloques, las características y opciones de diseño de las arquitecturas cambiaron significativamente, como se explica en las secciones siguientes.

Público o privado

La cadena de bloques de Bitcoin es una estructura de datos públicos, conocida por ser "inmutable". Para respaldar el control del doble gasto, la cadena de bloques conserva todas las transacciones pasadas de Bitcoin, sin restricciones sobre quién puede leer el historial. Pero cuando se contemplaron por primera vez las aplicaciones empresariales para la tecnología de la cadena de bloques, la consideración principal fue la confidencialidad, y así, algunas de las primeras divisiones de la cadena de bloques fueron cadenas de bloques *privadas* de varias formas, con controles de acceso sobre quién puede leer o escribir el registro. Existen numerosas sutilezas con respecto a los permisos de la cadena de bloques, que exploraremos a continuación.

"No confiable" o administrado

Las primeras cadenas de bloques se declararon "no confiables". La filosofía de la criptomoneda entre pares rechaza los bancos de reservas centrales, la supervisión de los gobiernos y toda la administración. El logro singular de la cadena de bloques original de Bitcoin fue permitir que extraños totales muevan valor real de forma confiable sin conocer nada de la otra parte, y sin utilizar a ningún tercero. La sabiduría convencional establece que el sistema de seguridad se basa en una triada de personas, procesos y tecnología. Las transacciones de Bitcoin son protegidas solo por la tecnología, y ese es el significado de "no confiable" en este contexto.[7]

La cadena de bloques original tampoco necesitaba la administración de claves criptográficas fuera de la cadena. La mayoría de los sistemas criptográficos requieren certeza sobre qué claves se asignan a cuáles usuarios (y qué metadatos de la clave, como la duración de la clave y el estado de revocación). Y necesitan la *administración del ciclo de vida de la clave* para renovar, revocar y reemplazar las claves de los usuarios según sea necesario. Pero Bitcoin no lo necesita. Los titulares de cuentas de Bitcoin se registran automáticamente (evitando alevosamente las reglas de identificación del cliente de los reguladores financieros) y aceptan la responsabilidad total por proteger sus monederos y

7 Por supuesto, cualquier software involucra procesos y personas a *nivel de diseño*. Los usuarios en general deben confiar en que los desarrolladores de software sepan lo que hacen, estén atentos y solucionen de inmediato las fallas o errores inevitables que surjan y se comprometan a una operación correcta y eficiente del sistema en general. O, si realmente no confiamos en un desarrollador de software, debemos confiar solamente en las garantías de un auditor independiente "confiable". Entonces, la confianza no se puede evitar en cierto nivel, y considerando esta advertencia, "no confiable" es una descripción adecuada de la *operación* esencialmente automática de las cadenas de bloques públicas y la falta de relación requerida entre las partes que realizan transacciones en estas criptomonedas.

claves privadas. Todos están solos; si pierde la clave de su monedero de Bitcoin, no hay personas ni procesos que garanticen su depósito o lo ayuden a recuperarla.

Los casos de uso más allá de la criptomoneda son mucho más complejos. Por un lado, habitualmente requieren *permisos*, porque no es normalmente aceptable que los registros corporativos sean públicos, y las empresas habitualmente no contratan externamente sus operaciones y mantenimiento de software a voluntarios anónimos. Los permisos de lectura y escritura de una cadena de bloques administrada requieren la clase de administración que Bitcoin eliminó para sus fines. Cuando debe recuperarse la administración, diferentes algoritmos de consenso de la "prueba de trabajo" de Bitcoin pueden ser más eficientes, y el sistema puede concentrarse en apenas unos pocos nodos en lugar de distribuirse en miles. El requisito de Bitcoin para un libro totalmente distribuido, sin una fuente de autoridad centralizada, simplemente no funciona para numerosos casos de uso empresariales o corporativos.

Otro factor para cadenas de bloques híbridas administradas proviene de la realidad de que los casos de uso de IAM de mayor riesgo con frecuencia necesitan terceros confiables para validar las identidades o atributos de los usuarios. La cadena de bloques original no admite la validación externa de declaraciones, sino que está construida simplemente con el propósito de proporcionar un libro distribuido verificable y prácticamente inmutable.[8]

El objetivo principal de las cadenas de bloques públicas originales, es llegar al consenso sobre un libro en ausencia de un administrador, puede volverse irrelevante si, después de todo, un tercero recibe una función central en el sistema. Parte de los desarrollos recientes de la cadena de bloques enfocados en la IAM han seguido el examen detallado de las cadenas de bloques disponibles y el hallazgo de que no cumplen las necesidades de la gestión de identidades.

Descentralizado o concentrado

Las redes distribuidas masivas de las cadenas de bloques arquetípicas de criptomoneda proporcionan una gran flexibilidad y redundancia. Una de las suposiciones de diseño que respalda la cadena de bloques original es que una simple mayoría de los nodos de la red siempre se mantendrá independiente; en consecuencia, una de las vulnerabilidades de Bitcoin se conoce como el "ataque del cincuenta y un por ciento"[9], en cuyo caso el registro se puede interferir, específicamente al distorsionar el consenso de manera encubierta.[10] Como se mencionó anteriormente, las cadenas de bloques más enfocadas en las empresas, como R3 Corda[11] y Hyperledger Fabric[12], no están masivamente distribuidas sino *concentradas*, y operan de forma privada. En lugar de asumir que una mayoría de los nodos se mantendrá sin corromper, la seguridad en las cadenas de bloques privadas requiere enfoques más convencionales, IBM por ejemplo implementa su cadena de bloques como servicio como un grupo de nodos virtuales, que se puede ejecutar físicamente en una

8 Vea el análisis de "Declaraciones/Atributos/Afirmaciones" en la Sección 4 más arriba.

9 https://en.bitcoin.it/wiki/Weaknesses#Attacker_has_a_lot_of_computing_power

10 Recuerde que con las cadenas de bloques públicas, el "consenso" se alcanza sobre el orden de entradas y la veracidad general del libro; un ataque del cincuenta y un por ciento en principio puede ver el libro manipulado, pero existen otras formas de crear transacciones fraudulentas, como tomar el control del monedero del titular de una cuenta y sus claves privadas.

11 http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services

12 https://hyperledger.org/projects/fabric
https://www.ibm.com/developerworks/cloud/library/cl-top-technical-advantages-of-hyperledger-fabric-for-blockchain-networks/index.html

computadora general, con medidas de protección que incluyen módulos de seguridad del hardware, contenerización y operadores altamente investigados (confiables)[13].

"Inmutabilidad"

Es una de las propiedades tradicionales de las cadenas de bloques originales. Es cierto que el esfuerzo requerido para subvertir una red de cadena de bloques pública y luego falsificar y volver a instalar todo el historial de bloques es completamente inviable.[14] Esta resistencia extrema a la manipulación es un medio para el fin de resistir el doble gasto, ya que, de acuerdo con la filosofía de Bitcoin, la comunidad debe poder consultar cada transacción realizada, sin el beneficio de un registro central de transacciones. Para la comunidad de Bitcoin, el costo de mantener un libro descentralizado es aceptado como el precio pagado por un sistema de moneda libre de bancos centrales y reguladores (con el algoritmo de consenso de la "prueba de trabajo", el costo se traduce directamente en enormes cargas de cómputo y el consumo de energía). Sin embargo, en otras aplicaciones, el enorme gasto incurrido por las cadenas de bloques *públicas* puede ser desproporcionado, y las medidas tradicionales de resistencia a la manipulación pueden ser adecuadas. También se debe señalar que la inmutabilidad de las cadenas de bloques públicas es calificada por el poder conservado por los equipos de mantenimiento de software para crear ramas (u "horquillas") mediante actualizaciones de software, que pueden inactivar los registros antiguos desde la fecha de la horquilla.

Tecnologías y autenticación de las cadenas de bloques

Actualmente observamos una variedad de ideas sobre los métodos de entrega de los atributos y mecanismos para comprobar su procedencia. Por una década o más, los marcos clásicos de federación[15] anticiparon que las *autoridades de atributos* operarían junto con los *proveedores de identidades* (IdPs) y brindarían información sobre los atributos en tiempo real. Un enfoque alternativo es equipar a los usuarios finales con tiendas de datos personales o monederos de atributos, basados en la nube o en dispositivos móviles, y coordinar que los detalles correspondientes se transmitan más o menos directamente a los proveedores de servicio (SP) bajo demanda.

Y ahora las cadenas de bloques proporcionan otro tipo de plataforma para distribuir atributos**.** Una ventaja de las numerosas cadenas de bloques, especialmente las instancias públicas, es la capacidad de descubrimiento. Su naturaleza distribuida y software transparente de fuente abierta, instalado en todo el mundo, significa que encontrar los registros es sencillo y no requiere un directorio general o esquema de direcciones.[16]

13 http://www-03.ibm.com/press/us/en/pressrelease/51840.wss

14 Sin embargo, manipular directamente un libro no es el único medio de ataque. Se debe señalar que, en las palabras del líder de seguridad Bruce Schneier, solo los aficionados buscan atacar la tecnología; los delincuentes profesionales atacan a las personas. Ninguna cadena de bloques es inmune a los ataques, por ejemplo, a las claves de usuarios individuales; la inmutabilidad de los datos escritos en una cadena de bloques no impide que se formen transacciones fraudulentas fuera de la cadena y se inyecten en el libro. https://www.schneier.com/crypto-gram/archives/2000/1015.html

15 Consulte, por ejemplo el "Sistema de identidades" fundacional de Microsoft https://www.identityblog.com/?p=355, la Estrategia nacional estadounidense para identidades confiadas en el ciberespacio de NSTIC https://obamawhitehouse.archives.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace, y el programa GOV.UK Verify, https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify.

16 Se debe señalar que encontrar registros de una cadena de bloques pública es una cosa, pero interpretarlos es otra. Con las criptomonedas, las transacciones y su significado son simples, pero cuando se almacena información más compleja en las entradas de cadenas de bloques, la semántica debe trabajarse en representación de todos los usuarios. El ajuste de reglas tiende a requerir una autoridad de política central, que es algo que los primeros diseños de cadenas de bloques especialmente buscaron erradicar. La interoperabilidad semántica de los registros de cadenas de bloques en casos de uso complejos como la IAM requiere una consideración atenta.

Se debe señalar en este punto que la transparencia de las cadenas de bloques públicas crea tensiones con los principios de privacidad. La arquitectura original de Bitcoin expone cada entrada en la cadena de bloques al mundo, por lo que la supervisión del sistema de monedas podría contratarse externamente; todo el historial de las transacciones debe estar disponible para que todos los vean. Cuando estos tipos de cadenas de bloques tienen un propósito inicial para aplicaciones como la IAM, los controles de privacidad se vuelven necesarios, como cifrar por separado las cargas de transacciones antes de segmentarse o referenciarse de las entradas de cadenas de bloques o aplicar capas adicionales de control de acceso al algoritmo nativo de la cadena de bloques para restringir quién puede leer (o escribir) el libro. Se presentan otros desafíos a la privacidad, como la exclusividad de los pares de claves de los titulares de cuentas. Cada transacción realizada con una cuenta se registra de forma permanente; una clave o "dirección" de Bitcoin podría no tener nombre y, como tal, ser anónima, pero forma un índice permanente (o "mango de correlación") del historial propio de la cadena de bloques y presenta un riesgo importante a la privacidad. Se pueden encontrar registros mediante una clave en particular y correlacionarlos con un perfil en particular.

Un tema especial en IAM se ha destacado especialmente con los conceptos de la cadena de bloques: *identidad autosoberana (Self Sovereign Identity,* SSI). Los defensores de SSI rechazan el control estricto habitualmente ejercido por los gobiernos y grandes empresas sobre las identidades de ciudadanos y clientes y requieren una mayor autodeterminación la forma en que las personas se presentan y revelan en línea, y la descentralización de la emisión de identidades. Sin embargo, para algunos casos de uso de mayor riesgo, se requiere una autoridad externa confiable para validar las declaraciones o afirmaciones. El objetivo y los principios de SSI no son nuevos y la mayoría afectan la cadena de bloques, pero se han unido al surgimiento de los libros distribuidos prácticos inspirados por las primeras cadenas de bloques públicas. La calidad de "autosoberanía" evoca la propiedad literal o metafórica de identidades por parte de las personas involucradas, y la recuperación del control.[17] La descentralización y disponibilidad de las cadenas de bloques son consideradas por muchos como una buena opción para SSI, y actualmente se está realizando una gran cantidad de investigación y desarrollo; vea por ejemplo la *Sovrin Foundation*[18] y su nuevo algoritmo sobre consenso *Plenum* que se enfoca en la confiabilidad de ciertos atributos, en especial en relación con el gráfico propio en línea. También se realiza importante investigación y desarrollo en la *Distributed Identity Foundation*[19] para administrar los metadatos de IAM como el estado de revocación, y por el proyecto *Rebooting Web of Trust* para distribuir claves públicas sin utilizar autoridades centrales, y reducir así los puntos únicos de falla.[20]

## Elementos importantes de las cadenas de bloques

Si evalúa soluciones posibles de IAM con cadenas de bloques o realiza su propia investigación y desarrollo original en gestión de identidades, debe analizar las siguientes cuestiones. Con fines de autenticación y autorización, las siguientes propiedades de las tecnologías de la cadena de bloques son especialmente importantes:

17 El movimiento de Identidad Autosoberana tiene mucho en común con la gestión de relaciones de proveedores (Vendor Relationship Management, VRM); vea https://cyber.harvard.edu/projectvrm/Main_Page

18 https://sovrin.org

19 http://identity.foundation

20 http://www.weboftrust.info/

**Disponibilidad y flexibilidad:** Las cadenas de bloques públicas se distribuyen masivamente y son casi universalmente accesibles (deben ser altamente disponibles para respaldar constantemente sus criptomonedas). La sincronización y replicación se realizan automáticamente, y las cadenas de bloques mantienen un estado acordado del registro en todos los nodos.

**Capacidad de descubrimiento (de los atributos):** una de las capacidades más subestimadas de la cadena de bloques es la capacidad de descubrimiento. No se requieren esquemas complicados de dirección o directorios para alcanzar la mayoría de las cadenas de bloques; el software de todos los participantes sabe dónde está el libro. Esta capacidad de acceso puede ser útil para sistemas globalmente escalables de IAM; los atributos de los usuarios estarán disponibles las 24 horas en un lugar virtual uniforme. Por otro lado, **el significado semántico de los atributos en una cadena de bloques debe ser comprendido y acordado** ***fuera de la cadena (es decir, por separado)***. Si bien una cadena de bloques distribuida técnicamente está disponible para todos los usuarios, parece posible que comunidades separadas en el sistema amplio puedan tener sus propias interpretaciones únicas (o códigos de clasificación) de lo que significan sus atributos; por lo que la *interoperabilidad* semántica no se desprende necesariamente de la capacidad de descubrimiento.

## Orientación sobre tecnologías de cadena de bloques para la autenticación

El propósito de las cadenas de bloques de criptomonedas era alcanzar un consenso de mantenimiento de redes sin líderes sobre el estado de un libro, de forma tal que puedan realizarse transacciones confiables sin un administrador central. La descentralización es costosa, es un 'estado de alta energía' que requiere un esfuerzo constante para respaldarla. Los gastos fijos compartidos del algoritmo de consenso son el precio pagado por los usuarios de Bitcoin en la administración anterior. La mayoría de las aplicaciones de IAM son intrínsecamente diferentes del ideal descentralizado de criptomonedas.

**Considere los procesos fuera de la cadena.** Un sistema de gestión de identidades habitualmente cubre varios dominios, a fin de presentar información sobre los usuarios a los sistemas con los que interactúan. Deben tomarse decisiones sobre qué datos de identidad son relevantes, quién responde por ellos y cómo se mantienen actualizados. Estos procesos de diseño y operativos con frecuencia incluyen a terceros o autoridades de algún tipo, que pueden no funcionar con la descentralización de una cadena de bloques. Recuerde que las cadenas de bloques públicas utilizan enormes redes de cómputos intensos, principalmente como resultado de la suposición de que no participa ningún tercero o administrador. Si de hecho se requieren autoridades fuera de la cadena en un sistema de IAM, los arquitectos deben aceptar al menos cierto grado de administración central, y la filosofía de una cadena de bloques distribuida podría no ser tan importante o ventajosa.

**¿Sobre qué debe alcanzar el consenso?** El consenso ha sido un tema importante pero segmentado en la ciencia informática por muchos años, y numerosos algoritmos preceden la ahora famosa "prueba de trabajo" utilizada por las primeras cadenas de bloques[21]. Los diseñadores de bases de datos y desarrolladores de juegos han considerado por largo tiempo la cuestión de determinar qué ocurrió primero. Recuerde que con la criptomoneda y las cadenas de bloques más orientadas a las transacciones, el consenso se refiere al *orden de eventos*, a fin de resolver el doble gasto con un árbitro. Por otro lado, en la gestión de

21 https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-proof-of-work.

identidades, puede no existir el equivalente a un problema de "doble gasto". Fundamentalmente, la identidad no es tan transaccional como la moneda. Entonces, en los casos de uso de la IAM, dedique un tiempo a revisar de qué se trataría el consenso descentralizado, y en qué medida sería un factor.

Considere también los diferentes requisitos de seguridad y registro durante el ciclo de vida de la identidad. Cuando un usuario se inscribe en un sistema de IAM, se deben verificar y registrar ciertos datos sobre ellos (habitualmente) para acceder a ellos más adelante. Cuando el usuario debe acceder a un sistema, algunos de estos factores pueden necesitar presentarse a las contrapartes y ser comprobados por ellas en tiempo real. Ciertas transacciones requieren que la identidad del usuario u otros atributos se relacionan con artefactos digitales; los registros de auditoría deben mantenerse según varios estándares y consultarse más tarde con una integridad razonable. Todos estos tipos de actividades colocan diferentes demandas sobre los registros de IAM, ya sean directorios tradicionales o cadenas de bloques más nuevas. Una consideración especial es un retraso importante de tiempo derivado de algunos algoritmos de consenso. La cadena de bloques de Bitcoin reconocidamente toma *en promedio* unos 10 minutos en actualizar el libro, lo que puede restringir el tiempo de respuesta de ciertas operaciones del ciclo de vida de identidad.

Considere la administración del ciclo de vida de la clave (es decir, en general, asegurarse de que las claves adecuadas estén el as manos adecuadas y permanezcan allí) es esencial para la mayor parte de la gestión de identidades, pero irrelevante para las primeras plataformas de cadenas de bloques. Con Bitcoin, nadie debe preocuparse con quién realizan una transacción, y el sistema no necesita establecer ninguna garantía sobre la custodia de claves privadas, ni la asociación de claves públicas con ciertas personas. Solo por este motivo, la unión de la IAM con las cadenas de bloques públicas puede crear un esfuerzo inútil: no es obvio que la descentralización del consenso sea útil cuando se requiere cierta autoridad para la gestión de claves. Las tecnologías más nuevas de cadenas de bloques específicas de la IAM deben prestar atención a esta necesidad de controles fundamentalmente más fuertes del ciclo de vida de las claves que los requeridos por las primeras cadenas de bloques.

Considere la seguridad de las claves privadas. Con la gestión de claves se relaciona el problema específico de las claves privadas del usuario final. El sistema de cadena de bloques de Bitcoin reconocidamente no se interesa en cómo sus usuarios finales cuidan sus claves públicas (es decir, sus monederos de criptomonedas). Una vez que se hizo evidente que las claves privadas pueden ser extraviadas o robadas por piratas informáticos, surgió un robusto mercado de soluciones de monederos, incluidas tiendas de claves basadas en la nube, almacenamiento en teléfonos móviles, servicios de respaldo y módulos personales de seguridad de hardware. En las cadenas de bloques más avanzadas, la gestión de claves del hardware también se está convirtiendo en un punto de interés.

Mantenimiento de la cadena de bloques. Uno de los puntos más destacados de diferencia entre las primeras cadenas de bloques y sus descendientes es la gestión del software central. Las cadenas de bloques públicas tienden a ser mantenidas por voluntarios de fuente abierta, en tanto que algunas de las plataformas más nuevas son cerradas o exclusivas (o al menos pueden comenzar así antes de ser de fuente abierta). Si bien el objetivo de la fuente abierta tiende a ser la dominación, una inquietud práctica de algunos implementadores de IAM empresarial es la dependencia en el mantenimiento del software.

Cuando surgen fallas o mejoras urgentes en el diseño, las empresas pueden desear certidumbre sobre cuándo se implementarán estas soluciones. Con la cadena de bloques de Bitcoin, ciertos problemas de diseño tomaron años en resolverse: con Ethereum, una falla importante condujo a una decisión unilateral del fundador de "dividir" esa cadena de bloques, lo que generó múltiples registros incompatibles y variaciones de la moneda.[22]

## Conclusión

Las tecnologías de cadenas de bloques son colectivamente un trabajo en progreso. A pesar de la emoción inicial sobre sus promesas generales de seguridad, en una inspección más detallada encontramos que las cadenas de bloques públicas originales en general no son una buena opción para la gestión de identidades y acceso. El objetivo de la criptomoneda (intercambiar dinero electrónico sin intermediarios y sin confianza) es fundamentalmente diferente del de la IAM empresarial, que típicamente requiere una administración mucho más rigurosa del ciclo de vida de las claves y controles de acceso que los ofrecidos por las cadenas de bloques públicas. Por otro lado, varios nuevos desarrollos de la tecnología de cadena de bloques prometen mejorar aspectos particulares de la IAM, como la procedencia de los atributos de identidad y las claves. Recomendamos que cualquier examen continuo de las tecnologías de cadenas de bloques para identidad comiencen con una declaración clara del problema y una apreciación de los inconvenientes en la seguridad de la cadena de bloques.

22 https://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds.

## Referencias y otras lecturas

"Want to really understand how bitcoin works? Here's a gentle primer"
https://arstechnica.com/tech-policy/2017/12/how-bitcoin-works/

"Immutable agreement for the Internet of value," Sigrid Seibold y George Samman, KPMG, 2016 https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf

"Blockchain plain and simple," Steve Wilson, Constellation Research, 30 de enero de 2017
https://www.constellationr.com/blog-news/blockchain-plain-and-simple

"Blockchain Security for Digital Identity" Adam Migus, septiembre de 2016
https://medium.com/@amigus/blockchain-Security-for-digital-identity-e10c8750cf9c

Decentralized Identity Foundation - DIF
http://identity.foundation

"Corda: An Introduction," Richard Gendal Brown, James Carlyle, Ian Grigg y Mike Hearn, R3, 2016 https://docs.corda.net/_static/corda-introductory-whitepaper.pdf

"Overview of Swirlds Hashgraph," Leemon Baird, Swirlds, 2016
http://www.swirlds.com/wp-content/uploads/2016/06/2016-05-31-Overview-of-Swirlds-Hashgraph-1.pdf

"Still don't understand blockchain? Let's untangle the wires"
https://www.weforum.org/agenda/2017/11/blockchain-bitcoin-ethereum-tech-explained/

"Do You Need a Blockchain?," Morgan E. Peck, IEEE Spectrum, septiembre de 2017
https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain

"Introduction to Identity Management"
https://meetings.internet2.edu/media/medialibrary/2014/11/06/20141028-dors-intro-to-idm.pdf

Online Identity: Who, Me?
https://www.internetsociety.org/resources/doc/2016/online-identity-who-me/

Recursos sobre identidad de Internet Society
https://www.internetsociety.org/issues/identity/